CLAIMS

Having thus described my invention, what I claim as new and desire to secure by Letters Patent is as follows:

1. A security device for installation at a node of a digital network, said security device comprising

a security/encryption engine for providing user transparent communications to another node of said digital network, and

a programmed data processor including embedded security policy manager functions for

detecting communications which include characteristics which differ from characteristics of normal usage and sending an alarm to said security/encryption engine for communication to another node as said user transparent communications and for responding to user transparent communications from another node of said digital network to control routing of communications in said digital network.

2. A security device as recited in claim 1, further including a memory for storing information corresponding to said user transparent communication,

3. A security device as recited in claim 1, wherein said routing of communications isolates a node of said digital network.

4. A security device as recited in claim 3, wherein said control of communications to isolate a node of said digital network is performed in real time.

5. A security device as recited in claim 1, wherein said node and said another node are hierarchically arranged locally in said digital network.

6. A security device as recited in claim 1, further including

means for defining a secure session between said node and said another node.

7. A security device as recited in claim 6, wherein said means for defining a secure session includes means for transmitting information corresponding to one of an authenticated user and an identification of a communicating node.

8. A security device as recited in claim 1, wherein said characteristics which differ from characteristics of normal usage are characteristics of a potential attack.

9. A security device as recited in claim 1, wherein said characteristics which differ from characteristics of normal usage correspond to a fault at a node or link of said digital network.

10. A security device as recited in claim 1 wherein said programmed data processor includes a manager object and at least one managed object corresponding to each connected node.

11. A digital network comprising

at least two locking devices at each of a plurality of nodes of said digital network,

a security policy manager device for detecting network communications or activity having some characteristics different from characteristics of normal usage and providing a signal to another network node, and

means responsive to a user transparent signal from another node for controlling said at least two locking devices to isolate a node selecting redundant communication paths in said digital network to maintain network communications between other network nodes.

12. A digital network as recited in claim 11, further including a memory for storing information corresponding to said user transparent communication,

13. A digital network as recited in claim 11, wherein said control of said locking devices to isolate a node of said digital network is performed in real time.

14. A digital network as recited in claim 11, wherein said node and said another node are hierarchically arranged locally in said digital network.

15. A digital network as recited in claim 11, further including

means for defining a secure session between said node and said another node.

16. A digital network as recited in claim 15, wherein said means for defining a secure session includes means for transmitting information corresponding to one of an authenticated user and an identification of a communicating node.

17. A digital network as recited in claim 11, wherein said characteristics which differ from characteristics of normal usage are characteristics of a potential attack.

18. A digital network as recited in claim 11, wherein said characteristics which differ from characteristics of normal usage correspond to a fault at a node or link of said digital network.

19. A digital network as recited in claim 11 wherein said programmed data processor includes a manager object and at least one managed object corresponding to each connected node.

20. A method of operating a digital network including steps of

detecting communications having characteristics differing from characteristics of normal usage at a node of said digital network,

communicating a user transparent signal to another node responsive to said detecting step, and

controlling communications at said node from said another node with a user transparent signal.

21. A method as recited in claim 20, wherein said step of controlling communications includes steps of

isolating said node from said network to encapsulate said communications having characteristics differing from normal usage, and

routing other communications in said digital network through redundant links between nodes of said digital network.

22. A method as recited in claim 20, wherein said detecting step is performed by a managed object at a node of said digital network and said controlling step is performed responsive to a managed object at said another node of said digital network.

23. A method as recited in claim 20 wherein said detecting, communicating and controlling steps are performed in substantially real time.

24. A method as recited in claim 20, including a further step of defining a secure session between a plurality of pairs of connected nodes in a communication path in said digital network.